UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,479	12/04/2003	Mark Kraus	MS1-2715US	6237

22801 7590 05/30/2008
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
TRUVAN, LEYNNA THANH	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
05/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/727,479	**Applicant(s)** KRAUS ET AL.	
	Examiner Leynna T. Truvan	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 19 February 2008.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-5,7,8 and 10-34 is/are pending in the application.

4a) Of the above claim(s) 6 and 9 is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-5,7,8 and 10-34 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-5, 7-8, and 10-34 are pending.

Claims 6 and 9 are cancelled by applicant.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/19/2008 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-5, 7-8, and 10-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanderpool, et al. (US 5,781,773), and further in view of Cromer, et al. (US 6,684,326).

As per claim 1:

Vanderpool discloses a method of file system protection for a resource-sparing operating system image, comprising:

loading a resource-sparing operating system image into random access memory (RAM), the image including a catalog file embedded therein; **(col.11, lines 31-35)**

creating a first hash of the image; **(col.8, lines 5-15)**

extracting a second hash of the image from the catalog file; **(col.7, line 63 – col.8, line 40)**

comparing the first hash and the second hash; and **(col.8, lines 1-15 and see Cromer below - col.5, lines 43-46)**

[blocking use of the image to boot the computing device when the first hash and the second hash do not match], or ***(see Cromer below - col.5, lines 43-46)***

validating the use of the image to boot the computing device if the first hash and the second hash match. ***(see Cromer below - col.5, lines 36-42 and lines 48-63)***

The catalog file is interpreted as a list containing specific information (i.e. name, location, or hash algorithm). Vanderpool discloses digital audio and compressed video (image) may also be linked to the data record by listing number and copied to and stored in the subdirectories under a hash algorithm as a function of the listing number. Vanderpool discloses listing or directories of hash algorithms corresponding to a thumbnail image and its filenames reads on the claimed hash of the image from the catalog file. (col.7, line 63 – col.8, line 40). Vanderpool includes hashing of the images extracting a second hash of the image from the catalog file, but did not go further in details of a comparison/matching process. Thus, Vanderpool did not include blocking the use of the image to boot the computing device when the first hash and the second hash do not match.

Cromer disclose a method and system for performing an authenticated boot of a computer system wherein the boot process for a computer system attached to a network is authenticated to ensure authorized access to an operating system image (Cromer - col.1, lines 48-51 and col.5, lines 63-65). Cromer disclose a pre specified list of bootable devices is presented to the user for selection and a determination of the selected device whether it contains an image of a desired operating system (Cromer - col.5, lines 22-35). Cromer discloses comparing the decrypted received hash to a list of authorized operating system boot record hashes (Cromer - col.5, lines 55-56). Based on the whether the received hash matches an authorized hash, the system then boots or halts appropriately (Cromer - col.5, lines 59-62). The list of authorized operating system boot record hashes is obviously the claimed second hash of the image from the catalog file because as established earlier, the catalog file is merely a listing of specific information. This reads on the claimed second hash of the image from the catalog file and blocking the use of the image to boot the computing device when the first hash and the second hash do not match. Further, Comer discusses hashing the boot record with a hash algorithm and determines if the system boots approves or not whereby a password is requested if the boot records are not approved. If the password is invalid, then the system is halted and if valid, then the system boots (Cromer - col.5, lines 40-47). Cromer includes validation of the first and second hash because Cromer's invention is to authenticate the boot process to ensure authorized access to an operating system image. Thus, avoids booting an incorrect operating system image (Cromer - col.5, lines 63-67). Therefore, discloses the claimed “*blocking use of the image to boot the computing device when the first hash and the second hash do not match* or validating the use of the image to boot the computing device if the first hash and the second hash match”.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Vanderpool with Cromer because this ensures the boot process for a computer system is authenticated to ensure authorized access to an operating system image which avoids booting an incorrect operating system image (Cromer - col.5, lines 55-67).

As per claim 2: see Cromer on col.5, lines 36-67; discussing the method of claim 1, wherein the comparing includes determining that the first hash and the second hash do not match, and wherein further the blocking the use of the image to boot the computing device if the first hash and the second hash do not match comprises determining an operational mode of the computing device is set to a run mode of operation.

As per claim 3: see Cromer on col.5, lines 36-67; discussing method of claim 1, wherein the comparing includes determining that the first hash and the second hash match, wherein further the validating the use of the image to boot the computing device if the first hash and the second hash match further includes validating a signature certification of the image.

As per claim 4: see Cromer on col.1, lines 53-57 and col.5, lines 11-67; discussing method of claim 1, further comprising evaluating a signature certification of the catalog file to determine if the signature certification of the catalog file is valid, and wherein the blocking the use of the image to boot the computing device if the first hash and the second hash do not match further includes blocking the use of the image to boot the computing device if the signature certification of the catalog file cannot be validated.

As per claim 5: see Cromer on col.1, lines 53-57 and col.5, lines 11-67; discussing method of claim 4, further comprising determining an operational mode of the computing device is set to a run mode of operation.

As per claim 6: Cancelled.

As per claim 7: see Cromer on col.5, lines 36-67; discussing method of claim 1, further comprising extracting first make and model attributes from the catalog file, comparing the first make and model attributes from the catalog file with second make and model attributes of the computing device, and wherein the blocking the use of the image to boot the computing device if the first hash and the second hash do not match further includes blocking the use of the image to boot the computing device when the first make and model attributes do not match the second make and model attributes.

As per claim 8: see Cromer on col.5, lines 55-67; discussing method of claim 7, further comprising determining an operational mode of the computing device is set to a run mode of operation.

As per claim 9: Cancelled.

As per claim 10: see Cromer on col.3, lines 22-26; discussing method of claim 1, further comprising booting the computing device from a prior image already loaded in flash memory of the computing device.

As per claim 11:

Vanderpool discloses a method of file system protection for a resource-sparing operating system image, the image including a catalog file embedded therein, comprising:

examining the catalog file and the image to determine if the image is a properly released image; and **(col.11, lines 31-35)**

[blocking use of the image to boot the computing device when the examining determines that the image is not a properly released image]. ***(see Cromer below - col.5, lines 43-46)***

The catalog file can broadly interpret as a list containing specific information (i.e. name, location, or hash algorithm). Vanderpool discloses digital audio and compressed video (image) may also be linked to the data record by listing number and copied to and stored in the subdirectories under a hash algorithm as a function of the listing number. Vanderpool discloses listing or directories of hash algorithms corresponding to a thumbnail image and its filenames reads on the claimed hash of the image from the catalog file. (col.7, line 63 – col.8, line 40). Vanderpool includes hashing of the images extracting a second hash of the image from the catalog file, but did not go further in details of a comparison/matching process. Thus, Vanderpool did not include blocking the use of the image to boot the computing device when the first hash and the second hash do not match.

Cromer discloses a method and system for performing an authenticated boot of a computer system wherein the boot process for a computer system attached to a network is authenticated to ensure authorized access to an operating system image (Cromer - col.1, lines 48-51 and col.5, lines 63-65). Cromer discloses a pre specified list of bootable devices is presented to the user for selection and a determination of the selected device whether it contains an image of a desired operating system (Cromer - col.5, lines 22-35). Cromer discloses comparing the decrypted received hash to a list of authorized operating system boot record hashes (Cromer - col.5, lines 55-56). Based on the whether the received hash matches an authorized hash, the system then boots or halts appropriately (Cromer - col.5, lines 59-62). The list of authorized operating system boot record hashes is obviously the claimed second hash of the image from the catalog file because as established earlier, the catalog file is merely a listing of specific information. This reads on the claimed second hash of the image from the catalog file and blocking the use of the image to boot the computing device when the first hash and the second hash do not match. Further, Comer discusses hashing the boot record with a hash algorithm and determines if the system boots approves or not whereby a password is requested if the boot records are not approved. If the password is invalid, then the system is halted and if valid, then the system boots (Cromer - col.5, lines 40-47). Cromer includes validation of the first and second hash because Cromer's invention is to authenticate the boot process to ensure authorized access to an operating system image. Thus, avoids booting an incorrect operating system image (Cromer - col.5, lines 63-67). Therefore, discloses the claimed "*blocking use of the image to boot the computing device when the first hash and the second hash do not match*".

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Vanderpool with Cromer because this ensures the boot process for a computer system is authenticated to ensure authorized access to an operating system image which avoids booting an incorrect operating system image (Cromer - col.5, lines 55-67).

As per claim 12: see Cromer on col.11, lines 31-35; discussing method of claim 11, wherein the step of examining is initiated upon a request to update the image, the method further including the step of loading an update image into random access memory (RAM).

As per claim 13: see Cromer on col.5, lines 15-18; discussing method of claim 1 l, wherein the step of examining is initiated upon a reset of the device.

As per claim 14: see Vanderpool on col.7, line 63 – col.8, line 40 and Cromer on col.5, lines 55-67; discussing method of claim 11, wherein the examining comprises: creating a first hash of the image; extracting a second hash of the image from the catalog file; and comparing the first hash and the second hash, and wherein a mismatch provides an indication that the image is not a properly released image.

As per claim 15: see Cromer on col.5, lines 15-67; discussing method of claim 14, further comprising determining an operational mode of the device.

As per claim 16: see Vanderpool on col.7, line 63 – col.8, line 40 and Cromer on col.1, lines 53-57 and col.5, lines 11-67; discussing the method of claim 11, wherein examining comprises: extracting a signature certification from the catalog file; validating the signature certification; and wherein failure of the step of validating the signature certification provides an indication that the image is not a properly released image.

As per claim 17: see Cromer on col.5, lines 55-67; discussing method of claim 16, further comprising the determining an operational mode of the device.

As per claim 18: see Vanderpool on col.7, line 63 – col.8, line 40 and Cromer on col.5, lines 22-35 and 55-67; discussing the method of claim 11, wherein the examining comprises: extracting first make and model attributes from the catalog file; comparing first make and model attributes from the catalog file to second make and model attributes of the device; and wherein a mismatch between the first and the second make and model attributes provides an indication that the image is not a properly released image for the device.

As per claim 19: see Cromer on col.5, lines 15-35; discussing method of claim 18, further comprising the determining an operational mode of the device.

As per claim 20: see Vanderpool on col.11, lines 31-36; discussing method of claim 11, further comprising loading the image into random access memory (RAM) of the device, and wherein the examining is processed after the loading.

As per claim 21: see Cromer on col.3, lines 22-26 and 60-62; discussing method of claim 11, wherein when the step of examining determines that the image is a properly released image, the method further comprising the steps of: erasing a previous image from flash memory of the device; programming the flash memory of the device with the properly released image.

As per claim 22: see Vanderpool on col.7, line 63 – col.8, line 40 and Cromer on col.1, lines 53-57 and col.5, lines 11-67; discussing the method of claim 11, wherein examining comprises: creating a first hash of the image; extracting a second hash of the image from

the catalog file; comparing the first hash and the second hash; extracting a signature certification from the catalog file; validating the signature certification; and extracting first make and model attributes from the catalog file; comparing first make and model attributes from the catalog file to second make and model attributes of the device; and
wherein any one of a first mismatch between the first hash and the second hash, a failure of the step of validating the signature certification, and a second mismatch between the first and the second make and model attributes provides an indication that the image is not a properly released image for the device.

4. Claims 23-25, 27-30, and 32-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott, et al. (US 6,615,329), in view of Neufeld (US 7,237,126).

As per claim 23:

Scott discloses a portable computing device, comprising:

flash memory, the flash memory including a protected area and an unprotected area; **(col.6, lines 11-14 and col.9, 7-15)**

a bootloader stored in the protected area of flash memory, the bootloader containing a crypto module; **(col.4, lines 29-31 and col.7, lines 47-55)**

an operating system image stored in the unprotected area of flash memory; random access memory (RAM); and **(col.7, lines 58-65)**

wherein the crypto module of the bootloader is operative to examine an image update *[to determine if the image update should be programmed into the unprotected area of flash* *memory to boot the device based on information included in a signed catalog file embedded in the image update].* **(See Neufeld on col.4, lines 3-30 and col.5, lines 37-57)**

Scott teaches a protected area of the flash memory and an unprotected area of the flash memory (col.6, lines 11-14 and col.9, 7-15). Scott discloses checking the state of the write authorization flag to determine whether the writes to the protected area have been properly authorized (col.3, lines 38-42). Although, Scott discloses examining an image update but did not clearly explain to determine if the image update should be programmed into the unprotected are of the flash memory to boot the device based on information included in the signed catalog file embedded in the image update.

Neufeld discusses the concern of the protection of reprogrammable start up memory of important subsystems embedded in the computer from unauthorized reprogramming or alteration of the computer's non-volatile memory (col.1, lines 35-38 and 54-63). Neufeld discusses the flashable or reprogrammable components may be protected using digital signature where the firmware may contain a protected segment which is generally not flashable or reprogrammable. This segment or "Boot Block" may be used to validate the integrity of the subsystem's memory prior to allowing it to execute (col.1, line 64 - col.2, line 2). Neufeld discloses that if the Boot Block or the firmware image that will be used to update the EEPROM is compromised in some way, that there is no method of validating the correctness of the program the subsystem will execute (col.2, lines 23-28). Thus, Neufeld's invention allows independent updating of both the Boot Block and firmware while providing the integrity of the software. It is possible that an unauthorized or corrupted version of firmware could be flashed into the subsystems EEPROM memory prior to executing the compromised software and can verify its correctness prior to flashing it into the EEPROM (col.2, lines 30-45). Therefore, Neufeld suggests determine if the image update should be programmed into the unprotected area of the flash memory to boot the device based on information included in a signed catalog file embedded in the image update.

It would have been obvious for a person of ordinary skills in the art o combine the teachings of Scott and Neufeld because allowing the update of the image while providing the integrity of the software where it is possible that an unauthorized or corrupted version of firmware could be flashed into the subsystems EEPROM memory prior to executing the compromised software and can verify its correctness prior to flashing it into the EEPROM (Neufeld on col.2, lines 30-45).

As per claim 24: see Neufeld on col.2, lines 30-45; discussing device of claim 23, wherein the crypto module programs the image update into the unprotected area of flash memory when the device is in test mode.

As per claim 25: see Scott on col.7, lines 6-20 and Neufeld on col.4, lines 3-30 and col.5, lines 37-57; discussing device of claim 23, wherein the bootloader stores the image update in the RAM until the crypto module determines that the image update should be programmed into the unprotected area of flash memory to boot the device.

As per claim 27: see Neufeld on col.4, lines 36-50 and col.5, lines 37-57; discussing device of claim 25, wherein the crypto module extracts a signature certification from the catalog file and attempts to validate the signature certification, the crypto module blocking use of the image update when the signature certification cannot be validated.

As per claim 28: see Neufeld on col.4, lines 36-50 and col.5, lines 37-57; discussing device of claim 25, wherein the crypto module extracts make and model attributes from the catalog file and compares them to make and model information for the device, the crypto module blocking use of the image update when the make and model attributes of the image update do not match the make and model attributes of the device.

As per claim 29: see Scott on col.3, lines 43-54 and Neufeld on col.4, lines 36-50; discussing device of claim 25, wherein the bootloader erases a current device image from the unprotected area of flash memory and programs the image update into the unprotected area of flash memory when the crypto modules determines that the image update may be used to boot the device.

As per claim 30: see Neufeld on col.5, lines 1-17; discussing device of claim 23, wherein a second crypto module of a Mira shell is operative upon a reset of the device to examine the installed operating system image to determine if the installed operating system image should be used to boot the device based on information included in a signed catalog file embedded in the installed operating system image.

As per claim 32: see Neufeld on col.4, lines 36-50 and col.5, lines 37-57; discussing device of claim 30, wherein the crypto module in the Mira shell extracts a signature certification from the catalog file and attempts to validate the signature certification, the crypto module in the Mira shell blocking use of the installed operating system image when the signature certification cannot be validated.

As per claim 33: see Neufeld on col.4, lines 36-50 and col.5, lines 37-57; discussing device of claim 30, wherein the crypto module in the Mira shell extracts make and model attributes from the catalog file and compares them to make and model information for the device, the crypto module in the Mira shell blocking use of the installed operating system image when the make and model attributes of the installed operating system image do not match the make and model attributes of the device.

As per claim 34: see Neufeld on col.4, lines 36-50 and col.5, lines 1-30; discussing device of claim 30, wherein the crypto module in the Mira shell allows the installed operating system image to be used to boot the device when the device is in test mode.

5. Claims 26 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scott, et al. (US 6,615,329) and Neufeld (US 7,237,126) combination and in further view of Cromer.

As per claim 26: *as rejected in view of Scott and Neufeld with the same rationale as claim 23 in* discussing device of claim 25. However, Scott and Neufeld combination did not discuss wherein the crypto module calculates a first hash of the image update, extracts a second hash from the catalog file, and compares the first hash and the second hash, the crypto module blocking use of the image update when the first hash and the second hash do not match.

Cromer discloses a method and system for performing an authenticated boot of a computer system wherein the boot process for a computer system attached to a network is authenticated to ensure authorized access to an operating system image (Cromer - col.1, lines 48-51 and col.5, lines 63-65). Cromer discloses a pre specified list of bootable devices is presented to the user for selection and a determination of the selected device whether it contains an image of a desired operating system (Cromer - col.5, lines 22-35). Cromer discloses comparing the decrypted received hash to a list of authorized operating system boot record hashes (Cromer - col.5, lines 55-56). Based on the whether the received hash matches an authorized hash, the system then boots or halts appropriately (Cromer - col.5, lines 59-62). The list of authorized operating system boot record hashes is obviously the claimed second hash of the image from the catalog file because as established earlier, the catalog file is merely a listing of specific information. This reads on the claimed second hash of the image from the catalog file and blocking the use of the image to boot the computing device when the first hash and the second hash do not match. Further, Comer discusses hashing the boot record with a hash algorithm and determines if the system boots approves or not whereby a password is requested if the boot records are not approved. If the password is invalid, then the system is halted and if valid, then the system boots (Cromer - col.5, lines 40-47). Cromer includes validation of the first and second hash because Cromer's invention is to authenticate the boot process to ensure authorized access to an operating system image. Thus, avoids booting an incorrect operating system image (Cromer - col.5, lines 63-67). Therefore, discloses the claimed "*blocking use of the image to boot the computing device when the first hash and the second hash do not match* or validating the use of the image to boot the computing device if the first hash and the second hash match".

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Vanderpool with Cromer because this ensures the boot process for a computer system is authenticated to ensure authorized access to an operating system image which avoids booting an incorrect operating system image (Cromer - col.5, lines 55-67).

As per claim 31: as rejected with same rationale as in claim 26; discussing device of claim 30, wherein the crypto module in the Mira shell calculates a first hash of the install operating system image, extracts a second hash from the catalog file, and compares the first hash and the second hash, the crypto module in the Mira shell blocking use of the image update when the first hash and the second hash do not match.

Response to Arguments

6. Applicant's arguments filed 2/19/2008 have been fully considered but they are not persuasive.

Regarding claims 1-22:

Examiner traverses the argument on pg.19, that Vanderpool does not discloses images of resource-sparing operating system images nor compress catalog file.

Applicant has mention that resource-sparing operating system is well known in the art is often implemented in computing device that have limited storage and memory resources. Vanderpool suggests such resource-sparing operating system with compressing the image and computer system have at least 16 Mbytes of RAM memory. This suggest a computing device having limited storage and memory resources (col.7, lines 15-18 and col.11, lines 31-35). Further, applicant indicated Vanderpool's images are in standard JPEG format. However, Vanderpool merely explains the compression/decompression process which performs decompression similar to a JPEG format (col.11, lines 36-41). Vanderpool does not insinuate the images are only in JPEG format.

Vanderpool suggests creating a first hash of the created image (col.8, lines 4-15) and a second hash of the image from the catalog file where the second image obviously is a stored has that will be used as a reference to during the comparison process (col.8, lines 35-40). Innuendo, Cromer also suggests first and second hash. Thus, the Vanderpool and Cromer combination obviously teaches the claimed invention.

As per the argument on pg.20, where Vanderpool fails to disclose blocking the use of the image to boot the computing device when the first hash and the second hash do not match is traversed. Cromer is combined with Vanderpool to teach this limitation. Cromer disclose a method and system for performing an authenticated boot of a computer system wherein the boot process for a computer system attached to a network is authenticated to ensure authorized access to an operating system image (col.1, lines 48-51 and col.5, lines 63-65). Cromer disclose a pre specified list of bootable devices is presented to the user for selection and a determination of the selected device whether it contains an image of a desired operating system (col.5, lines 22-35). Comer discusses hashing the boot record with a hash algorithm and determines if the system boots approves or not whereby a password is requested if the boot records are not approved. Thereafter, if the password is invalid, then the system is halted (col.5, lines 40-47). Further, Cromer discloses comparing the decrypted received hash to a list of authorized operating system boot record hashes (col.5, lines 55-56). Based on the whether the received hash matches an authorized hash, the system then boots or halts appropriately (col.5, lines 59-62). The list of authorized operating system boot record hashes is obviously the claimed second hash of the image from the catalog file because as established earlier, the catalog file is merely a listing of specific information. This reads on the claimed second hash of the image from the catalog file and blocking the use of the image to boot the computing device when the first hash and the second hash do not match. Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Vanderpool with the teach of blocking the use of the image to boot the computing device when the first hash and the second hash do not match as taught by Cromer because this ensures the boot process for a computer system is authenticated to ensure authorized access to an operating system image which avoids booting an incorrect operating system image (col.5, lines 55-67).

All dependent claims are also rejected by virtue of the dependency

7. Applicant's arguments, see RCE, filed 2/19/2008, with respect to Applicant Arguments have been fully considered and are persuasive.

Claims 23-34 are now rejected over Scott and Neufeld combination.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135